

2-22-00

A

02/17/00

1 IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

2 Inventorship..... Malvar et al.
 3 Applicant..... Microsoft Corporation
 3 Attorney's Docket No. MS1-338US
 4 Title: System and Method for Protecting Data Streams in Hardware Components

5 TRANSMITTAL LETTER AND CERTIFICATE OF MAILING6 To: Commissioner of Patents and Trademarks,
7 Washington, D.C. 202318 From: Lewis C. Lee (Tel. 509-324-9256; Fax 509-323-8979)
9 Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201JC530 U.S. PTO
09/507478
02/17/0010 The following enumerated items accompany this transmittal letter and are being submitted for the
matter identified in the above caption.

11 1. Specification—title page, plus 34 pages, including 57 claims and Abstract
 2. Transmittal letter including Certificate of Express Mailing
 3. 8 Sheets Formal Drawings (Figs. 1-9)
 4. Return Post Card

14 Large Entity Status [x]

Small Entity Status []

15 Date: 2/17/00

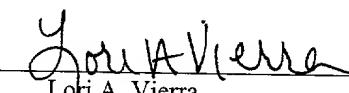
By:

Lewis C. Lee
Reg. No. 34,65617 CERTIFICATE OF MAILING

18 I hereby certify that the items listed above as enclosed are being deposited with the U.S. Postal
 Service as either first class mail, or Express Mail if the blank for Express Mail No. is completed below, in
 an envelope addressed to The Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the
 below-indicated date. Any Express Mail No. has also been marked on the listed items.

20 Express Mail No. (if applicable) EL47251885121 Date: 2/11/00

By:



Lori A. Vierra

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**System and Method for Protecting Data Streams in
Hardware Components**

Inventor(s):

Henrique Malvar

Paul England

ATTORNEY'S DOCKET NO. MS1-338US

1 **TECHNICAL FIELD**

2 This invention relates to systems and methods for protecting data content,
3 such as audio and video data. More particularly, this invention relates to
4 protecting data streams in hardware components.

5 **BACKGROUND**

6 More and more content is being delivered in digital form online over
7 private and public networks, such as Intranets and the Internet. For a user, digital
8 form allows more sophisticated content and online delivery improves timeliness
9 and convenience. For a publisher, digital content also reduces delivery costs.
10 Unfortunately, these worthwhile attributes are often outweighed in the minds of
11 publishers by a corresponding disadvantage that online information delivery
12 makes it relatively easy to obtain pristine digital content and to pirate the content
13 at the expense and harm of the publisher.

14 Piracy of digital content, especially online digital content, is not yet a great
15 problem. Most premium content that is available on the Web is of low value, and
16 therefore casual and organized pirates do not yet see an attractive business stealing
17 and reselling content. Increasingly, though, higher-value content is becoming
18 available. Books and audio recordings are available now, and as bandwidths
19 increase, video content will start to appear. With the increase in value of online
20 digital content, the attractiveness of organized and casual theft increases.

21 The unusual property of content is that the publisher (or reseller) gives or
22 sells the *content* to a client, but continues to restrict *rights* to use the content even
23 after the content is under the sole physical control of the client. For instance, a
24 publisher will typically retain copyright to a work so that the client cannot

1 reproduce or publish the work without permission. A publisher could also adjust
2 pricing according to whether the client is allowed to make a persistent copy, or is
3 just allowed to view the content online as it is delivered. These scenarios reveal a
4 peculiar arrangement. The user that possesses the digital bits often does not have
5 full rights to their use; instead, the provider retains at least some of the rights. In a
6 very real sense, the legitimate user of a computer can be an adversary of the data
7 or content provider.

8 "Digital rights management" is therefore fast becoming a central
9 requirement if online commerce is to continue its rapid growth. Content providers
10 and the computer industry must quickly address technologies and protocols for
11 ensuring that digital content is properly handled in accordance with the rights
12 granted by the publisher. If measures are not taken, traditional content providers
13 may be put out of business by widespread theft or, more likely, will refuse
14 altogether to deliver content online.

15 Traditional security systems have not fully addressed this problem. There
16 are highly secure schemes for encrypting data on networks, authenticating users,
17 revoking certificates, and storing data securely. Fig. 1 shows a representative
18 prior art system 20 having a content producer/provider 22 that produces original
19 content (e.g., audio, video) and distributes the content over a network 24 to a client
20 26. The content producer/provider 22 has a content storage 30 to store digital data
21 streams of original content and a distribution server 32 that transfers the content
22 over the network 24 (e.g., Internet). The distribution server 32 includes an
23 encoder 34 that encrypts and compresses the data prior to distribution over the
24 network. In this manner, the data is protected in route over the public network 24.
25

1 The client 26 is equipped with a processor 40, a memory 42, and one or
2 more media output devices 44 (e.g., monitor, display, sound card, speakers, etc.).
3 The processor 40 runs various tools to process the data stream, such as tools to
4 decompress the stream, decrypt the data, filter the content, and apply controls
5 (tone, volume, etc.). An operating system 50 is stored in the memory 42 and
6 executes on the processor 40. The operating system 50 implements a media player
7 52 that is capable of playing streaming media content, including both audio and
8 video data. The media player 52 has a decoder 54 that provides the tools run by
9 the processor 40 to decompress and decrypt the content.

10 Once the content is stored on the machine, there are products designed to
11 restrict rights after purchase. For instance, a product from Liquid Audio
12 (www.liquidaudio.com) allows a content provider to restrict content to being
13 played only on one machine. The product secures the source material by keeping
14 an encrypted copy of the content on disk, and keeping a decryption key safely
15 somewhere.

16 While this architecture safely protects the content from the provider 22 to
17 the client 26 and even provides some protection while stored on the client, it does
18 not address the assurance of content security *after* the content has been delivered
19 to a client's operating system. Ultimately, useful content must be assembled
20 within the client machine for display or audio output, and again, at this point the
21 bits are subject to theft.

22 Fig. 2 shows client-side components to illustrate how raw data bits may be
23 stolen despite protections in delivery and storage of the content. Encrypted and
24 compressed data is received from the network at a communication port 60. The
25 data is passed to the media player 52, which implements

1 decryption/decompression tools 54 to decrypt and decompress the content stream.
2 The media player 52 outputs a pulse code modulated (PCM) data stream, which is
3 essentially the raw sequence of digitized samples without compression and
4 encryption.

5 The media player 52 calls to an operating system API (application program
6 interface) layer 62 to submit the PCM data to a mixer 64 (or other processing
7 component). The mixer may be implemented, for example, using ACM (audio
8 compression manager) or DirectX technology from Microsoft Corporation. The
9 mixer 64 processes the PCM data with other sources to produce a desired output.
10 At this point, the processed data is passed to a driver 66 (software and/or
11 hardware) which outputs the data to the media output device(s) 44, such as a
12 sound card and speaker, or a display.

13 With this traditional architecture, the data is left unprotected throughout the
14 operating system software and hardware of the client device. Regardless of the
15 upstream encryption and compression, the data is eventually passed to the lower
16 level software and hardware components in a clear (unencrypted) form, which can
17 be stolen. For instance, an attacker might introduce a fake driver 72 to receive the
18 data from the mixer 64 and store the raw data on a storage medium 74 for illicit
19 use that is not contemplated by the content provider (e.g., redistribution, multiple
20 plays, etc.). Suppose, for example, that the media player is implemented using
21 DirectX API layers. DirectX is an open standard that allows software applications
22 to read sound and video data. A software package (e.g., “Total Recorder”
23 software package) can install itself as if it were a sound card driver (i.e., fake
24 driver 72) and all audio or video that flows into this virtual sound driver can be
25 captured into a standard sound file (e.g. in “.wav” format).

1 Accordingly, there is a need for an architecture that protects bits after they
2 have been given to the operating system. It is also desirable that the architecture
3 integrate with an existing multimedia processing system called “DirectX” from
4 Microsoft Corporation, which runs atop Windows brand operating systems. The
5 DirectX architecture defines how to control and process streams of multimedia
6 data using modular components called *filters*. Examples of filters include
7 compressors, decompressors, renderers, mixers, parsers, splitters, and tuners for
8 both audio and video data types. The filters have input or output pins, or both, and
9 are connected to each other in a configuration called a *filter graph*. Applications
10 use an object called the *filter graph manager* to assemble the filter graph and
11 move data through it. The filter graph manager provides a set of Component
12 Object Model (COM) interfaces so that applications can access the filter graph.
13 Applications can directly call the filter graph manager interfaces to control the
14 media stream or retrieve filter events, or they can use the media player control to
15 play back media files. The reader is directed to the Microsoft web site
16 Microsoft.com, and the file path for “directx” for more background information on
17 DirectX, filter graphs, and individual filters.

18 One of the main attractions to the DirectX architecture is that it is modular
19 and extensible. Unfortunately, these same advantageous attributes may be
20 manipulated for improper use. For instance, thief may insert a “T” into the filter
21 graph to siphon compressed or uncompressed data to disk.

22 One possible approach is to secure the filter graph and the device drivers
23 using only certified components. The drawback with this approach is that it
24 introduces the burden of obtaining certificates for components and authenticating
25 them during use.

1 Another approach is to keep the data encrypted until it reaches the driver
2 layer 66. This approach has a drawback in that it may lead to poor quality output
3 because some processing results from the filters do not transfer cleanly through the
4 decryption algorithm when the encrypted data is subsequently decrypted,
5 oftentimes rendering the data unrecoverable. Consider, for example, an encrypted
6 MPEG stream. It will lose the MPEG transport layer framing and the filter graph
7 will be unable to handle it. Another example is PCM audio. If the encrypted
8 audio is mixed with another signal (e.g., a “ding” from a mail program),
9 decryption is impossible. As a final example, a volume control that multiplies an
10 encrypted audio bit stream by a constant renders an encrypted stream
11 unrecoverable.

12 Thus, there is a need for an architecture that protects data while in the
13 operating system and hardware components of the computer and integrates with
14 the DirectX architecture, without deterioration of the signal quality when played.

15

16 SUMMARY

17 This invention concerns an architecture for protecting data streams in the
18 operating system and hardware components of a computer.

19 In one implementation, a server serves encrypted and compressed content
20 over a network to a client. The client receives the content and decrypts and
21 decompresses it. At this point, the content is in the form of a pulse code
22 modulated (PCM) data stream, which is essentially the raw sequence of digitized
23 samples without compression and encryption. The PCM data stream is ready for
24 processing (e.g., adjusting volume, mixing other sources, etc.). The client

1 implements a set of tools to process the PCM data, such as filter graph
2 technologies at the operating system level.

3 To prevent theft of the raw bits while they are being processed, the client
4 scrambles the PCM data. One technique is to add noise by adding a random signal
5 to the content. More particularly, the client has a scrambler to produce periodic
6 sets of deterministic tone patterns. The scrambler modulates the amplitude of the
7 tone patterns based on a first key, thereby embedding the first key into the
8 modulated tone patterns. The scrambler also generates a random signal based on
9 the first key and a second key. The tone patterns and random signal are added to
10 the PCM data to scramble the content.

11 The scrambled content is passed to a filter graph or other processing
12 system. The content is processed while in its scrambled state. Any attacker
13 attempting to siphon off the bits while being processed in the filter graph will
14 capture only noisy data, which is worthless for redistribution or copying purposes.

15 After processing, the scrambled data is passed to a driver for output. The
16 driver implements a descrambler to unscramble the content by subtracting out the
17 noise. The descrambler detects the tone patterns in the content and recovers the
18 first key from the varying amplitudes of the tone patterns. The descrambler also
19 receives the second key via a separate channel (e.g., a cryptographically secured
20 path) and generates the same random signal based on the recovered first key and
21 the second key. The descrambler subtracts the tone patterns and the random signal
22 from the scrambled content to restore the PCM data to an unscrambled state, but
23 with the modifications resulting from the processing.

24 In another implementation, the server scrambles the content prior to
25 distribution over the network. The server-based scrambler cooperates with, or is

1 integrated into, a compressing unit that compresses the content so that the
2 compression algorithm does not render the scrambled content unrecoverable.

3

4 **BRIEF DESCRIPTION OF THE DRAWINGS**

5 The same numbers are used throughout the drawings to reference like
6 elements and features.

7 Fig. 1 is a block diagram of a prior art client-server network system in which
8 the server provides encrypted and compressed content over a network (e.g.,
9 Internet) to a client.

10 Fig. 2 is a block diagram of prior art hardware and software components
11 implemented at the client to decrypt, decompress, and play the content.

12 Fig. 3 is a block diagram of a client architecture that employs scrambling
13 technology to protect data in the operating system and hardware components.

14 Fig. 4 is a block diagram showing one implementation of the scrambling
15 technology of Fig. 3.

16 Fig. 5 is a flow diagram of a scrambling process implemented by the
17 scrambling technology of Figs. 3 and 4.

18 Fig. 6 is a time domain representation of a modulated tone signal added to
19 the data as part of the scrambling process.

20 Fig. 7 is a time domain representation of random samples added to the data
21 as part of the scrambling process.

22 Fig. 8 is a block diagram of a tone detector and demodulator employed in
23 the scrambling technology of Fig. 4.

1 Fig. 9 is a block diagram of a client-sever network system implementing
2 the scrambling technology on a network level, wherein scrambling occurs at the
3 content provider and descrambling takes place at the client.

4

5 **DETAILED DESCRIPTION**

6 **Client-Based Architecture**

7 Fig. 3 shows a client-side architecture 100 that protects data streams (e.g.,
8 audio and video data) in the client computer. For discussion purposes, the client
9 may be implemented as a general purpose computing unit (e.g., desktop PC,
10 laptop, etc.) having a processor, volatile memory, non-volatile memory, and an
11 operating system. It may also be implemented as other devices, such as cable
12 modems, set-top boxes, audio/video appliances, and the like.

13 Fig. 3 shows a software/hardware architecture 100 implemented on the
14 client computer. It is assumed that the client implements a tamper-resistant
15 software application that connects to a content provider's server using an SSL
16 (secure socket layer) or other secure and authenticated connection to purchase,
17 store, and playback content. The tamper-resistant software stops attackers from
18 easily modifying this component or extracting keys. However, at some point the
19 audio must be handed to the operating system for playback.

20 The architecture 100 includes a communication layer or port 60 that
21 receives encrypted and compressed data from a server over a network. The data is
22 typically encrypted using well-know algorithms (e.g., RSA) and compressed using
23 well-known compression techniques (e.g., AVI, MPEG, ASF, WMA, MP3). The
24 data is passed to the media player 102, which is preferably implemented as the
25 “Windows Media Player” from Microsoft Corporation. The “Windows Media

1 "Player" is implemented using DirectX API (application programming interface)
2 layers, a group of technologies designed by Microsoft to make Windows-based
3 computers a suitable platform for running and displaying applications rich in
4 multimedia elements such as full-color graphics, video, 3-D animation, and
5 surround sound.

6 The media player 102 implements decryption/decompression tools 104 to
7 decrypt and decompress the content stream. At this stage, the content is in the
8 form of a pulse code modulated (PCM) data stream, which is essentially the raw
9 sequence of digitized samples without compression and encryption. To prevent
10 theft of the raw bits as underlying filters process them, the media player 102 also
11 implements a scrambler 106 to scramble the PCM data. The scrambler 106
12 modifies the data to such an extent that the bits, if stolen, would be essentially
13 useless. For instance, scrambled audio may have a large amount of noise that
14 sounds awful and cannot be removed, thereby negating any value in the stolen
15 data. Yet, at the same time, the scrambled version of the audio or video looks
16 sufficiently like real audio or video to the filters in the filter graph that normal,
17 unmodified decoders or signal processing components work well. Thus, the
18 scrambled content "looks like" unmodified content, but still guards against theft.

19 The scrambled PCM data is passed through an operating system API layer
20 62 to a filter graph 108, which processes the PCM data by adding one or more
21 other signals, adjusting volume or tone, and so forth. The filter graph 108
22 processes the scrambled PCM data as if the data were the original, unscrambled
23 PCM data. The filter graph 108 has one or more filters, such as a mixer, volume,
24 tone, encoder, render, and the like that process the PCM data. It is noted that the
25

1 filter graph 108 is shown for discussion purposes, but other types of signal
2 processing technologies may be substituted for the filter graph.

3 The processed data is passed to a driver 110, which may be implemented in
4 software and/or hardware. The driver 110 implements a descrambler 112 to
5 unscramble the scrambled PCM data and restore the PCM data to its pre-
6 scrambled condition, plus the modifications made as a result of the filter graph
7 processing. The descrambler 112 outputs the unscrambled, modified PCM data to
8 the media output device(s) 44.

9 The scrambler 106 and descrambler 112 utilize one or more secret keys 114
10 to generate the scrambling signal that is added to the PCM data. The keys 114
11 may be passed between the media player 102 and the driver 110 through an in-
12 band channel accompanying the scrambled data, and/or via an out-of-band channel
13 separate from the data path (e.g. the IOCTL device I/O control channel in
14 DirectX). One implementation of the media player 102 and driver 110, and the
15 keys utilized to scramble and unscramble PCM data, is described below in more
16 detail with reference to Fig. 4.

17 The scrambling architecture protects the content while it is being processed
18 by the operating system and lower level hardware components. An attacker
19 hoping to siphon off raw bits from the filter graph 108 using a fake driver 72
20 instead receives scrambled data that is worthless from a recording or redistribution
21 standpoint, thereby eliminating any financial incentive for the theft. Moreover, it
22 is very difficult to unscramble the data without knowledge of the keys 114.

1 **Scrambling Techniques**

2 There are different ways to implement the scrambling architecture at the
3 client to scramble the PCM data. One approach is to add noise to the signal. In
4 the audio context, one noise-addition scheme is to generate a set of speech, music
5 or noise-like functions using a session key and add those functions to the signal,
6 either directly in the time domain or in a frequency or wavelet domain. The
7 choice of function, its amplitude, phase, and dilation is selected on the basis of the
8 key generator. Adding a few tens of noise bursts per second renders the signal
9 worthless to an attacker, and the space that the attacker must “search” to remove
10 the noise is quite large, even if the attacker knows the noise basis. However, given
11 the key (and assuming no overloads) the noise signal can be subtracted exactly to
12 return to the unscrambled state.

13 An alternative approach, used in prior art, is to employ time-domain and
14 frequency-domain scrambling. In time-domain scrambling, the signal is broken
15 into frames (e.g., 2 or 3 seconds), and each frame is broken into several segments.
16 Within each frame, segments are permuted and reassembled. Typically, each
17 frame uses a different permutation. A secret key controls the sequence of
18 permutations. In frequency-domain scrambling, the signal is partitioned into
19 overlapping frames (e.g., 50 ms), which are then mapped to the frequency domain
20 via an FFT-based filter bank. The frequency bands are permuted and sent through
21 a synthesis filter bank. Again, a secret key controls the sequence of permutations.
22 Frequency-domain scrambling is harder to break than time-domain scrambling,
23 but has the disadvantage of the additional computations for the analysis and
24 synthesis filter banks.

1 The main disadvantage of time-domain and frequency-domain scrambling
2 is that the scrambled signal cannot go through a mixer (e.g. a filter graph mixer
3 such as 108 in Fig. 3), because after descrambling, the mixed signals would end up
4 being scrambled. The scrambling based on noise addition, described below,
5 overcomes this problem: signals mixed to the scrambled audio remain intact after
6 descrambling.

7

8 **Exemplary Noise-addition-based Scrambling**

9 Fig. 4 shows client-side components that implement a noise-addition-based
10 scrambling process to protect content while the content is being handled in the
11 operating system and hardware components of the client computer. More
12 particularly, Fig. 4 shows an exemplary implementation of the scrambler 100 at
13 the media player 102 and the descrambler 112 at the driver 110. The scrambling
14 process is described with additional reference to the flow diagram of Fig. 5. These
15 steps are performed by the various software and/or hardware components shown
16 in Fig. 4.

17 The process begins with the receipt of an encrypted and compressed data
18 stream (e.g., audio, video) at the media player 102 (steps 200 and 202). The media
19 player utilizes tools 104 to decrypt and decompress the stream, resulting in a PCM
20 data stream (step 204). The scrambler 106 scrambles the PCM data by adding
21 noise to the data (step 206). The scrambler 106 has a tone burst generator and
22 modulator 120 to generate a synchronization tone and a cryptographic pseudo
23 random number generator (PRNG) 122 to generate a random signal. Both the
24 sync tone and the random signal are added to the PCM data to produce noisy or
25 scrambled PCM data.

1 The tone burst generator 120 and PRNG 122 use two levels of keys to
2 create the sync tone and random signal: (1) an “in-band” key 124, and (2) an “out-
3 of-band” or “session” key 126. Both the tone burst generator 120 and the PRNG
4 122 use the in-band key 124, while only the PRNG 122 uses the out-of-band key
5 126. The keys may be implemented, for example, with large bit length, such as
6 56-bit or 128-bit keys.

7 The tone burst generator and modulator 120 uses the in-band key to
8 generate sets of tone bursts that can be easily recognized at the descrambler (step
9 208 in Fig. 5). The tone patterns are added periodically to the PCM data signal,
10 such as every 100 ms.

11 Fig. 6 shows an exemplary sync tone 300 having a deterministic pattern of
12 bursts of alternating plus/minus values. The bursts may have one of two different
13 amplitudes, such as +0.5/-0.5 or +1/-1. Modulating the amplitude of each burst
14 pattern allows the scrambler to encode one bit or piece of information per burst
15 sequence. For instance, one sequence of tone bursts 302 utilizes +1/-1 to represent
16 a first binary value (e.g., 1) and a different sequence of tone bursts 304 utilizes
17 +0.5/-0.5 to represent a second binary value (e.g., 0). The in-band key 124 is
18 embedded into the sets of tone burst sequences as an aggregate of the bits in order
19 to pass the key along with the data to the driver. The in-band key can be changed
20 with each audio/video clip, with sets of clips, or even within clips.

21 The sync tone 300 has a frequency that is preferably one-half the sampling
22 frequency of the original signal. For audio data with a sampling frequency of 44.1
23 kHz, the tone burst generator 120 generates a synchronization tone at 22.05 kHz.
24 The tone can be easily detected at the descrambler and removed. Alternatively,

1 even if the descrambler does not remove completely the sync tone, a digital-to-
2 analog converter used in the driver or sound card will remove this tone frequency.

3 With reference again to Figs. 4 and 5, the cryptographic PRNG 122
4 generates a pseudo random signal using the in-band key and the out-of-band
5 session key (step 210 in Fig. 5). Fig. 7 shows an exemplary random sequence 400
6 having a random pattern of data values with amplitudes of +1 or -1. The PRNG
7 122 is implemented to provide an equal chance of a +1 or -1 output, with the
8 overall average being zero to avoid introducing a DC shift to the original data
9 signal.

10 While the in-band key 124 is embedded into the tone sync signal, the
11 session key 126 is kept independent of the data and passed over a separate channel
12 128 from the data path. The session key 126 is protected using a cryptographic
13 key exchange (e.g., a Diffie-Hellman exchange and authentication) to ensure that
14 the key 126 is safely transported from the media player 102 to the driver 110 over
15 the channel 128 (which can be the IOCTL device control channel in DirectX, for
16 example). Accordingly, the scrambler 106 or media player 102 is equipped with
17 encryption and signing capabilities to encrypt and sign the session key for secure
18 transportation to the driver 110 and descrambler 112.

19 The scrambler 106 adds the sync tone bursts and the random signal to the
20 PCM data via adders 130 to scramble the data (step 212 in Fig 5). If desired, the
21 original signal (i.e., PCM data) and the random signal can be normalized to return
22 the composite signal to a range anticipated by the filter graph 108. For instance,
23 the PCM data may be multiplied by a factor 0.75 and the random signal may be
24 multiplied by a factor 0.25 prior to adding the two signals to normalize the
25 resulting composite signal.

1 The scrambled PCM data is passed to the filter graph 108 where it is
2 processed and mixed with other sources (step 214 in Fig. 5). The filter graph may
3 have one or more filters to process the data. As an example, the filter graph may
4 adjust the volume of the signal or may impose an arbitrary delay as part of a
5 processing step. The filters operate on the noisy data as if the data were the raw
6 PCM data. The filter graph outputs the modified noisy data to the driver 110.

7 At step 216 in Fig. 5, the descrambler 112 at the driver 110 descrambles the
8 modified noisy PCM data by removing the noise component from the data. The
9 descrambler 112 has a tone detector and demodulator 140, a cryptographic PRNG
10 142, and a hardware interface 144. The tone detector and demodulator 140 detects
11 the synchronization tone in the composite signal, measures any volume and delay
12 introduced by the filter graph 108, and demodulates the tones to recover the in-
13 band key 124 (step 218 in Fig. 5). The tone detector 140 passes the recovered in-
14 band key 124 to the PRNG 142.

15 The descrambler 112 also receives the session key 126 from the out-of-
16 band channel 128, decrypts and authenticates it, and gives the key 126 to the
17 PRNG 142. The descrambler is equipped with decryption and verification means
18 to decrypt and authenticate the session key as having been sent from the media
19 player 102. The PRNG 142 implements the same algorithm as that used in the
20 media driver's PRNG 122. Given the same in-band key 124 and session key 126,
21 the PRNG 142 recreates the same random signal that was previously added to the
22 PCM data at the media player (step 220 in Fig. 5).

23 The descrambler 112 subtracts the sync tone and random signal from the
24 noisy PCM data via subtractors 146 to remove the noise (step 222 in Fig. 5). The
25

1 PCM data is passed through the hardware interface 144 to the output devices (e.g.,
2 sound card, display) where the process ends (steps 224 and 226).

3 Fig. 8 shows one implementation of the tone detector and demodulator 140
4 implemented at the descrambler 112. The tone detector and demodulator has a
5 matched filter 500 to detect the sync tone in the noisy PCM data. The matched
6 filter 500 has as its impulse response $h(n)$ a finite-length, time reversed copy of the
7 pure sync tone. Therefore, the output $y(n)$ of the matched filter is given by

$$8 y(n) = \sum_{l=-L}^L h(l)x(n-l)$$

9

10
11 where $x(n)$ is a modified noisy data signal, and $2L+1$ is the length of the tone
12 bursts. When the position of the tone pattern $h(n)$ is aligned with the tone
13 components in the signal, $y(n)$ has a maximum. The position of the first maximum
14 determines the delay 506 by which the tone and PRNG noise patterns should be
15 moved in time in order to align properly with the modified noisy data.

16 The delay value and the noisy data are passed to a peak search module 502
17 that estimates any volume change imposed by the filter graph 108. The module
18 estimates the appropriate gain 508 (by which the regenerated tone bursts and
19 PRGN noise should be multiplied prior to the subtraction 146) through a search
20 procedure, in which a gain estimate is iteratively refined until the signal energy
21 after tone subtraction is minimized. The regenerated sync tone with the correct
22 gain and delay is produced in module 510.

23 Detection of the in-band key is performed by amplitude demodulation
24 module 512. For each tone burst, the module compares the burst amplitude with
25

1 the average tone burst amplitude measure over a few past intervals. If the
2 amplitude is above the average (say the amplitude is equal to 1.0 and the average
3 is 0.75), then a bit of the key is demodulated as having one binary value (say
4 “one”). If the amplitude is below that average (say the amplitude is equal to 0.5
5 and the average is 0.75), then a bit of the key is demodulated as having the other
6 binary value (say “zero”). The process is repeated for subsequent tone burst until
7 all bits of the in-band key 124 are recovered. The in-band key 124 can then be
8 used by the cryptographic PRNG 142 to regenerate the random noise sequence to
9 be subtracted from the scrambled signal.

10 In the above implementation, noise is introduced to the content by adding
11 both a sync tone and a random signal. Alternatively, the content may be
12 scrambled by XORing at least a portion of the content with a random bit stream
13 generated by the PRNG 122. For instance, for 16 bit audio, the least significant 13
14 bits are XORed with bits generated by the PRNG 122. This effectively scrambles
15 the content, with the additional property that one cannot “overflow” the integer
16 representing the sound. To descramble the content, the lower bits are once again
17 XORed with the same random bit stream.

18

19 **Conclusion**

20 The scrambling architecture is beneficial in that it protects the data content
21 while in the operating system and hardware components of the computer. Another
22 advantage is that the architecture integrates well with the existing DirectX
23 technology. Although the invention has been described in language specific to
24 structural features and/or methodological steps, it is to be understood that the
25 invention defined in the appended claims is not necessarily limited to the specific

1 features or steps described. Rather, the specific features and steps are disclosed as
2 preferred forms of implementing the claimed invention.

1 **CLAIMS**

2 1. A client comprising:

3 a processor;

4 a memory;

5 one or more output devices;

6 a content player stored in the memory and executed on the processor to
7 play content in the one or more output devices;

8 an operating system stored in the memory and executed on the processor,
9 the operating system having processing tools for processing the content in support
10 of the content player; and

11 a scrambling system to scramble the content before the content is processed
12 by the processing tools of the operation system and to unscramble the content after
13 the content is processed by the processing tools of the operation system.

14
15 2. A client as recited in claim 1, wherein the processing tools comprises
16 a filter graph with one or more filters that process the content.

17
18 3. A client as recited in claim 1, wherein the content player receives the
19 content in an encrypted and compressed format, the content player decrypting and
20 decompressing the content.

21
22 4. A client as recited in claim 1, wherein the scrambling system adds
23 noise to the content.

1 5. A client as recited in claim 1, wherein the scrambling system XORs
2 at least a subset of content with a random stream of bits.

3
4 6. A client as recited in claim 1, wherein the scrambling system
5 transforms the content using one of time-domain or frequency-domain scrambling.

6
7 7. A client as recited in claim 1, wherein the operating system has at
8 least one driver for the output devices and the scrambling system comprises:

9 a scrambler resident at the content player to scramble the content to
10 produce scrambled content; and

11 a descrambler resident at the driver to unscramble the scrambled content to
12 recover the content.

13
14 8. A client as recited in claim 1, wherein the scrambling system adds a
15 random signal to the content to produce scrambled content and subtracts the
16 random signal from the scrambled content to recover the content.

17
18 9. A client as recited in claim 1, wherein the scrambling system adds a
19 periodic sync tone and a random signal to the content to produce scrambled
20 content and subtracts the sync tone and the random signal from the scrambled
21 content to recover the content.

22
23 10. A client as recited in claim 1, wherein the scrambling system utilizes
24 at least one key to scramble the content.

1 **11.** A client as recited in claim 1, wherein the scrambling system
2 comprises:

3 a tone generator to create periodic sets of tone patterns having varying
4 amplitudes based on a first key;

5 a first random number generator to create a random signal based on the first
6 key and a second key;

7 an adder to add the tone patterns and the random signal to the content to
8 produce scrambled content;

9 a tone detector to detect the tone patterns in the scrambled content and
10 recover the first key from the varying amplitudes of the tone patterns;

11 a second random number generator to create a random signal based on the
12 recovered first key and the second key; and

13 a subtractor to subtract the tone patterns and the random signal from the
14 scrambled content to restore the content.

15
16 **12.** A client as recited in claim 11, wherein the second key is passed via
17 a channel separate from the scrambled content.

18
19 **13.** A client as recited in claim 11, wherein the second key is exchanged
20 between the first and second random number generator over a secured path.

21
22 **14.** A client as recited in claim 1, wherein the scrambling system is
23 implemented in software stored in the memory and executed on the processor.

1 **15.** A content scrambler for scrambling content, comprising:
2 a tone generator and modulator to create periodic sets of tone patterns and
3 to modulate amplitudes of the sets based on a first key;
4 a random number generator to create a random signal based on the first key
5 and a second key; and
6 an adder to add the sets of tone patterns and the random signal to the
7 content to produce scrambled content.

8
9 **16.** A content scrambler as recited in claim 15, wherein the tone
10 generator and modulator modulates the amplitudes in a way that embeds the first
11 key into the sets of tone patterns.

12
13 **17.** A content scrambler as recited in claim 15, wherein the tone
14 generator and modulator produces the tone patterns with one of two amplitudes,
15 wherein tone patterns with a first amplitude represent a first binary value and tone
16 patterns with a second amplitude represent a second binary value, the first key
17 being encoded into the sets of tone patterns as an aggregate of the first and second
18 binary values.

19
20 **18.** A content scrambler as recited in claim 15, wherein the second key
21 is encrypted for secure transportation to a descrambler.

22
23 **19.** A media player for playing multimedia content, comprising the
24 content scrambler of claim 15.

1 **20.** An operating system comprising the content scrambler of claim 15.

2
3 **21.** A content descrambler for unscrambling scrambled content,
4 comprising:

5 a tone detector and demodulator to detect periodic sets of tone patterns in
6 the scrambled content and to demodulate amplitudes of the sets to recover a first
7 key;

8 a random number generator to create a random signal based on the
9 recovered first key and a second key; and

10 a subtractor to subtract the tone patterns and the random signal from the
11 scrambled content to recover content.

12
13 **22.** A content descrambler as recited in claim 21, wherein the tone
14 patterns have one of two amplitudes so that tone patterns with a first amplitude
15 represent a first binary value and tone patterns with a second amplitude represent a
16 second binary value, the tone detector and demodulator using the first and second
17 binary values from the varying amplitudes to recover the first key.

18
19 **23.** A content descrambler as recited in claim 21, wherein the second
20 key is received separately from the scrambled content.

21
22 **24.** An operating system comprising the content scrambler of claim 21.

1 **25.** A scrambling architecture for protecting content distributed by a
2 content provider over a network to a client, comprising:

3 a content scrambler to scramble the content using first and second keys to
4 produce scrambled content, the scrambler embedding the first key into the
5 scrambled content and passing the second key separate from the scrambled
6 content;

7 a content descrambler to recover the first key from the scrambled content
8 and to receive the second key, the descrambler unscrambling the scrambled
9 content using the first and second keys to recover the content.

10
11 **26.** A scrambling architecture as recited in claim 25, wherein the
12 content scrambler and the content descrambler are implemented in software.

13
14 **27.** A scrambling architecture as recited in claim 25, wherein the
15 content scrambler is implemented at the content provider, so that the content is
16 scrambled prior to distribution over the network to the client.

17
18 **28.** A scrambling architecture as recited in claim 25, wherein the
19 content scrambler is implemented at the client, so that the content is scrambled at
20 the client after distribution over the network from the content provider.

21
22 **29.** A scrambling architecture as recited in claim 25, wherein the
23 content descrambler is implemented within an operating system at the client.

1 **30.** A scrambling architecture as recited in claim 25, wherein the
2 content descrambler is implemented within a driver at the client.

3
4 **31.** A scrambling architecture as recited in claim 25, wherein the
5 content scrambler passes the second key to the content descrambler over a
6 cryptographically secured path.

7
8 **32.** A scrambling architecture as recited in claim 25, wherein the
9 content scrambler comprises:

10 a tone generator and modulator to create periodic sets of tone patterns and
11 to modulate amplitudes of the sets based on the first key;

12 a random number generator to create a random signal based on the first and
13 second keys; and

14 an adder to add the sets of tone patterns and the random signal to the
15 content to produce the scrambled content.

16
17 **33.** A scrambling architecture as recited in claim 32, wherein the tone
18 generator and modulator modulates the amplitudes in a way that embeds the first
19 key into the sets of tone patterns.

1 **34.** A scrambling architecture as recited in claim 32, wherein the tone
2 generator and modulator produces the tone patterns with one of two amplitudes,
3 wherein tone patterns with a first amplitude represent a first binary value and tone
4 patterns with a second amplitude represent a second binary value, the first key
5 being encoded into the sets of tone patterns as an aggregate of the first and second
6 binary values.

7
8 **35.** A scrambling architecture as recited in claim 32, wherein the
9 content descrambler comprises:

10 a tone detector and demodulator to detect the periodic sets of tone patterns
11 in the scrambled content and to demodulate the amplitudes of the sets to recover
12 the first key;

13 a random number generator to create a random signal based on the
14 recovered first key and the second key; and

15 a subtractor to subtract the tone patterns and the random signal from the
16 scrambled content to recover the content.

17
18 **36.** A client-server system for protecting content, comprising:

19 a client;

20 a server to serve content to the client, the server having an encoder to
21 encrypt and compress the content to produce encoded content;

22 the client receiving the encoded content from the server and having a
23 decoder to decrypt and decompress the encoded content to recover the content;

1 the client having a scrambler to scramble the content after decryption and
2 decompression, the content remaining scrambled while processed by the client;
3 and

4 the client further having a descrambler to unscramble the content after
5 processing for subsequent playing.

6
7 **37.** A client-server system as recited in claim 36, wherein the client is
8 equipped with a media player to play the content, processing tools to support the
9 media player, and a driver; the scrambler being implemented as part of the media
10 player and the descrambler being implemented as part of the driver.

11
12 **38.** A client-server system as recited in claim 36, wherein the client runs
13 an operating system, and the content is scrambled while being handled by the
14 operating system.

15
16 **39.** A method for protecting content within a computer device,
17 comprising:

18 receiving encoded content;
19 decoding the encoded content to recover the content;
20 scrambling the content after the decoding;
21 processing the content while scrambled;
22 descrambling the content after the processing; and
23 playing the content.

1 **40.** A method as recited in claim 39, wherein the scrambling comprises
2 adding noise to the content.

3
4 **41.** A method as recited in claim 39, wherein the scrambling comprises
5 XORing at least a subset of the content with a random stream of bits.

6
7 **42.** A method as recited in claim 39, wherein the scrambling comprises
8 transforming the content using one of time-domain or frequency-domain
9 transforms.

10
11 **43.** A method as recited in claim 39, wherein the scrambling comprises:
12 adding sets of sync tones periodically to the content; and
13 adding a random signal to the content.

14
15 **44.** A method as recited in claim 43, wherein the descrambling
16 comprises:

17 detecting the sets of sync tones in the content;
18 subtracting the sync tones from the content; and
19 subtracting the random signal from the content.

20
21 **45.** A method as recited in claim 39, wherein the scrambling comprises:
22 producing periodic sets of tone patterns having varying amplitudes based
23 on a first key;
24 generating a random signal based on the first key and a second key; and
25 adding the tone patterns and the random signal to the content.

1
2 **46.** A method as recited in claim 45, wherein the descrambling
3 comprises:

4 detecting the tone patterns in the content;
5 recovering the first key from the varying amplitudes of the tone patterns;
6 generating a random signal based on the recovered first key and the second
7 key; and
8 subtracting the tone patterns and the random signal from the scrambled
9 content to restore the content.

10
11 **47.** A method as recited in claim 39, wherein the processing comprises
12 passing the content through a filter graph.

13
14 **48.** A computer-readable medium having computer-executable
15 instructions for performing the method of claim 39.

16
17 **49.** A method for delivering content from a server to a client over a
18 network, comprising:

19 encoding the content at the server;
20 serving the content from the server to the client;
21 decoding the content at the client;
22 scrambling the content after the decoding;
23 processing the content while scrambled;
24 descrambling the content after the processing; and
25 playing the content.

1
2 **50.** A method as recited in claim 49, wherein the scrambling comprises:
3 adding sets of sync tones periodically to the content; and
4 adding a random signal to the content.

5
6 **51.** A method as recited in claim 50, wherein the descrambling
7 comprises:

8 detecting the sets of sync tones in the content;
9 subtracting the sync tones from the content; and
10 subtracting the random signal from the content.

11
12 **52.** A method for delivering content from a server to a client over a
13 network, comprising:

14 scrambling the content at the server to produce scrambled content;
15 compressing the scrambled content at the server;
16 serving the compressed, scrambled content from the server to the client;
17 decompressing the compressed, scrambled content at the client to recover
18 the scrambled content;
19 processing the scrambled content;
20 descrambling the scrambled content after the processing to recover the
21 content; and
22 playing the content.

1 **53.** A method as recited in claim 52, wherein the scrambling comprises:
2 producing periodic sets of tone patterns having varying amplitudes based
3 on a first key;

4 generating a random signal based on the first key and a second key; and
5 adding the tone patterns and the random signal to the content.

6
7 **54.** A method as recited in claim 53, wherein the descrambling
8 comprises:

9 detecting the tone patterns in the content;
10 recovering the first key from the varying amplitudes of the tone patterns;
11 generating a random signal based on the recovered first key and the second
12 key; and
13 subtracting the tone patterns and the random signal from the scrambled
14 content to restore the content.

15
16 **55.** A computer-readable medium having computer-executable
17 instructions for:

18 producing periodic sets of tone patterns having varying amplitudes based
19 on a first key;
20 generating a random signal based on the first key and a second key; and
21 adding the tone patterns and the random signal to the content to scramble
22 the content.

1 **56.** A computer-readable medium as recited in claim 55 further having
2 computer-executable instructions for:

3 detecting the tone patterns in the content;

4 recovering the first key from the varying amplitudes of the tone patterns;

5 generating a random signal based on the recovered first key and the second
6 key; and

7 subtracting the tone patterns and the random signal from the scrambled
8 content to restore the content.

9
10 **57.** A computer-readable medium having computer-executable
11 instructions for:

12 detecting periodic sets of tone patterns within scrambled content, the tone
13 patterns having varying amplitudes that were modulated based on a first key;

14 recovering the first key from the varying amplitudes of the tone patterns;

15 generating a random signal based on the recovered first key and the second
16 key; and

17 subtracting the tone patterns and the random signal from the scrambled
18 content to produce unscrambled content.

1 **ABSTRACT**

2 A scrambling architecture protects data streams in the operating system and
3 hardware components of a computer by scrambling the otherwise raw data prior to
4 the data being handled by the operating system. The architecture has a scrambler
5 implemented at either the client or the server that adds noise to the content. More
6 specifically, the scrambler produces periodic sets of tone patterns having varying
7 amplitudes based on a first key. The scrambler also generates a random signal
8 based on the first key and a second key. The tone patterns and random signal are
9 added to the content to scramble the content. The scrambled content is then
10 passed to the filter graph (or other processing system) where the content is
11 processed while scrambled. Any attacker attempting to siphon off the bits during
12 processing will steal only noisy data, which is worthless for redistribution or
13 copying purposes. After processing, the scrambled data is passed to a driver for
14 output. The driver implements a descrambler to unscramble the content by
15 subtracting out the random noise signal. The descrambler detects the tone patterns
16 in the content and recovers the first key from the varying amplitudes of the tone
17 patterns. The descrambler also receives the second key via a separate channel
18 (e.g., a cryptographically secured path) and generates the same random signal
19 using the recovered first key and the second key. The descrambler subtracts the
20 tone patterns and the random signal from the scrambled content to restore the
21 content.

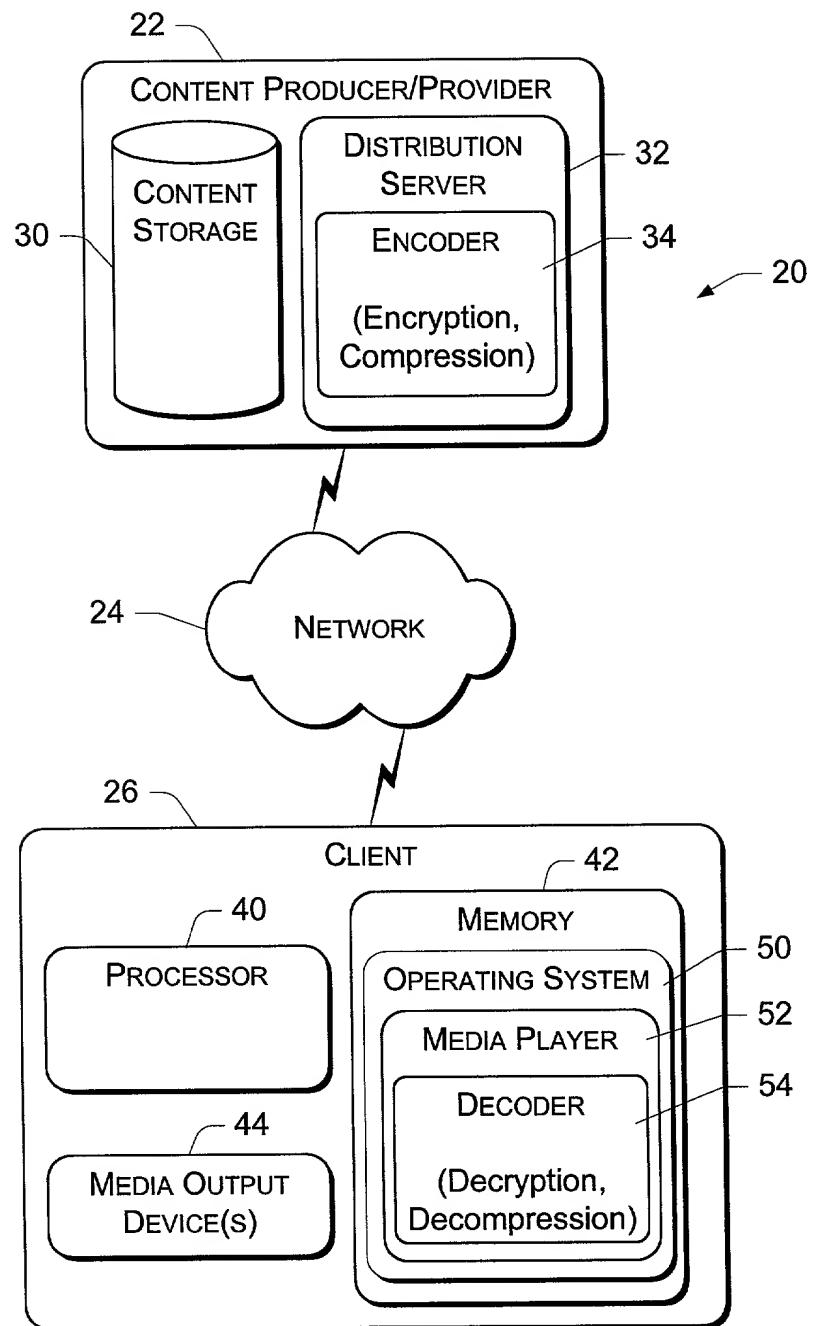


Fig. 1
Prior Art

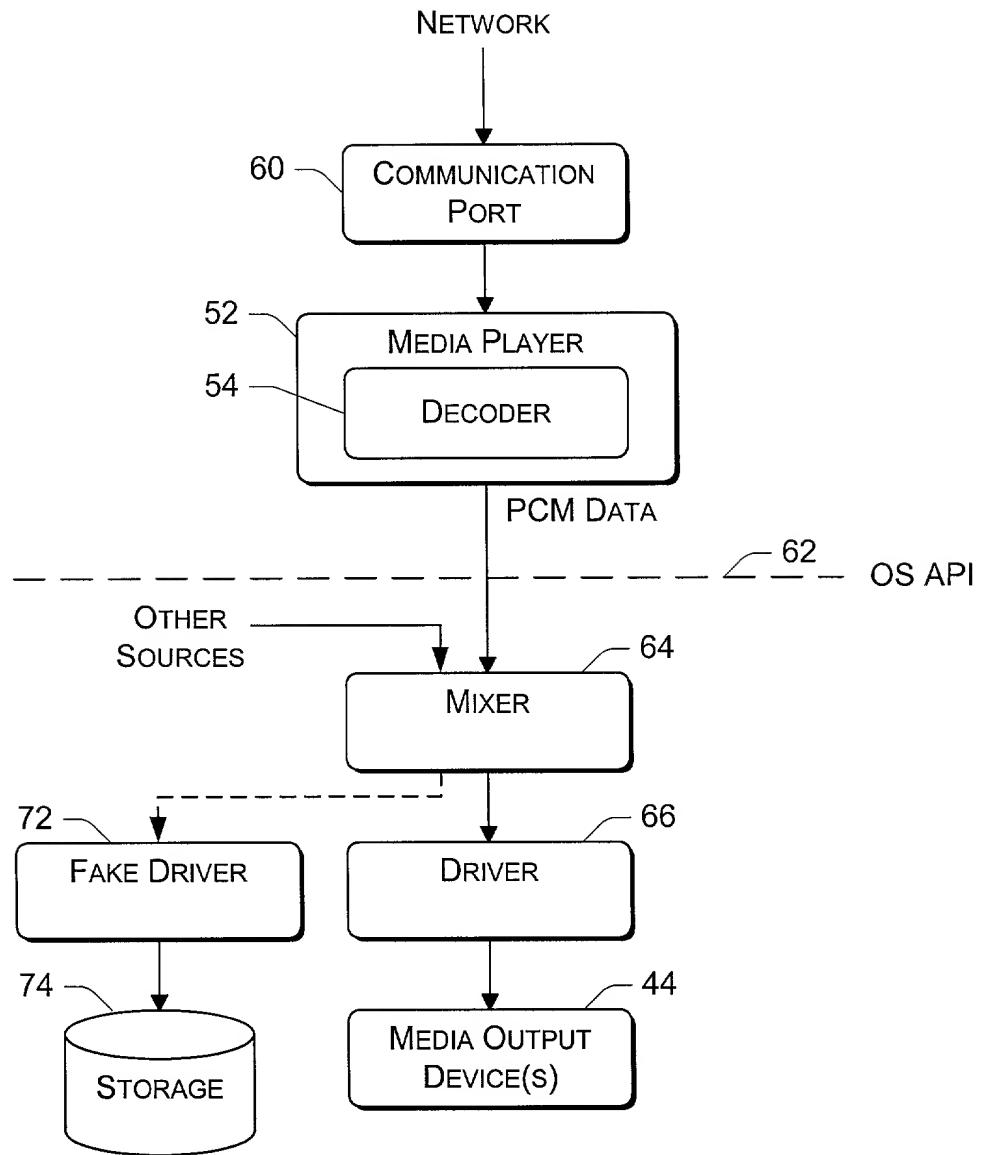


Fig. 2
Prior Art

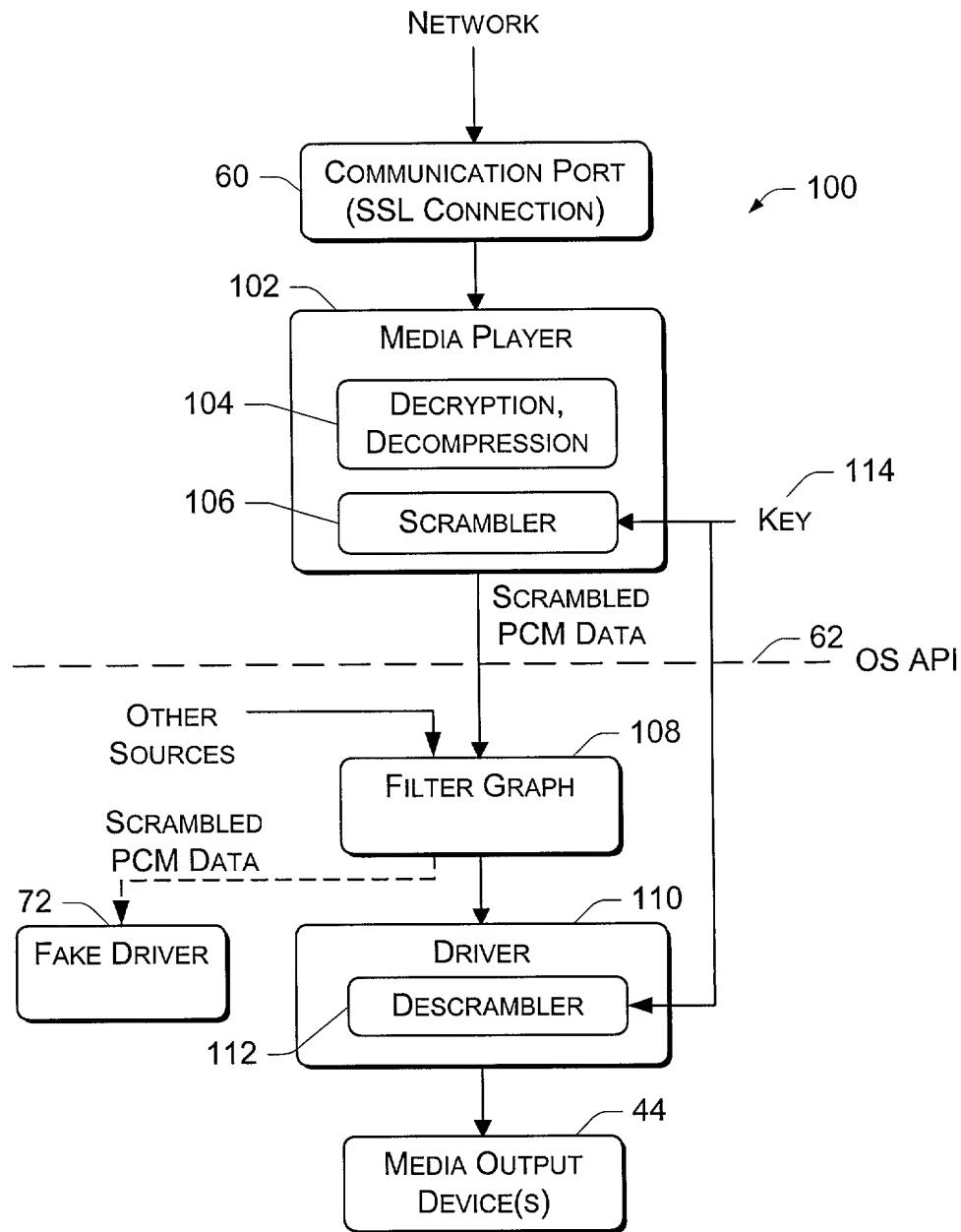


Fig. 3

20120920-22240560

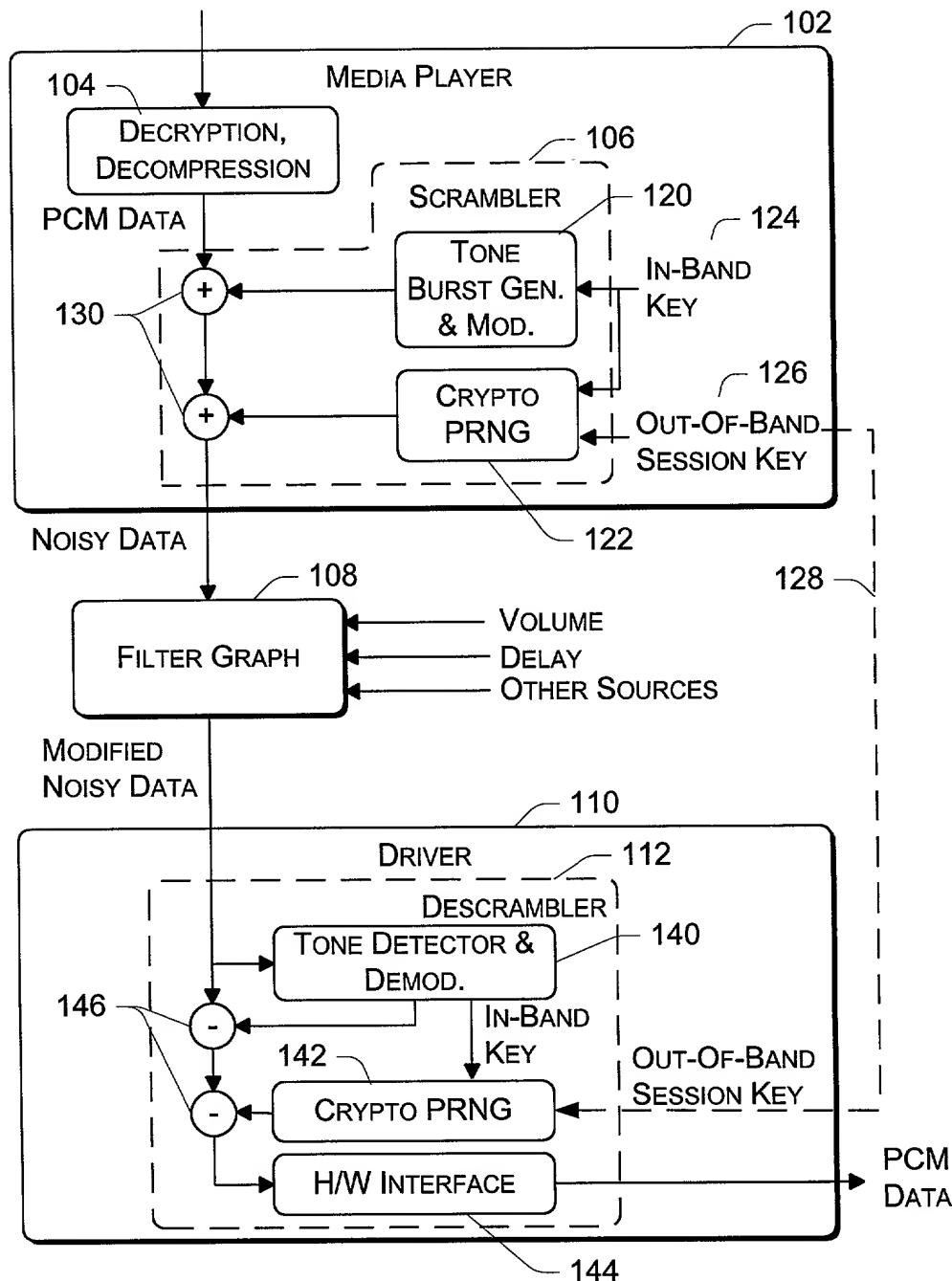


Fig. 4

00507126-0023-00

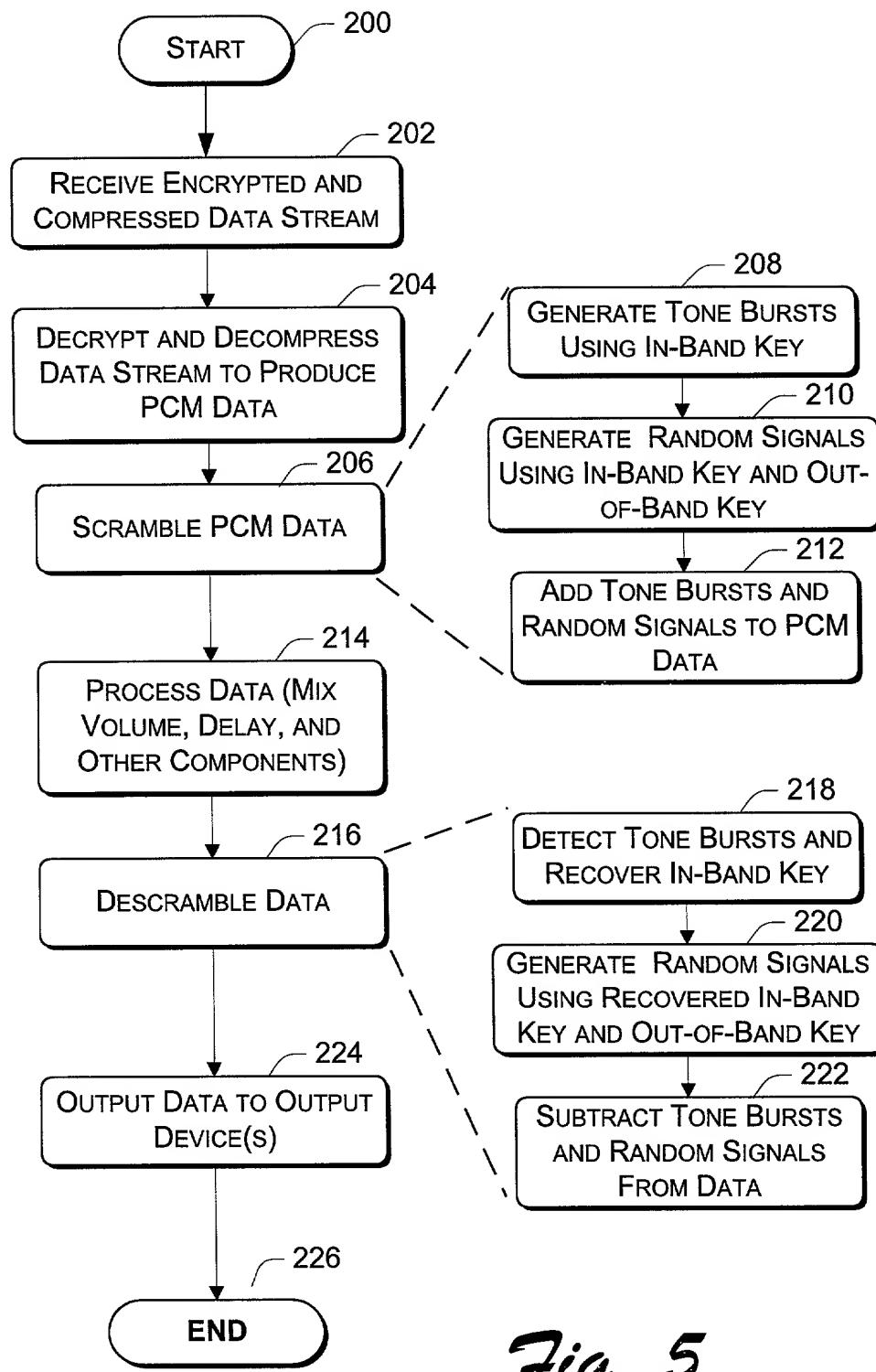


Fig. 5

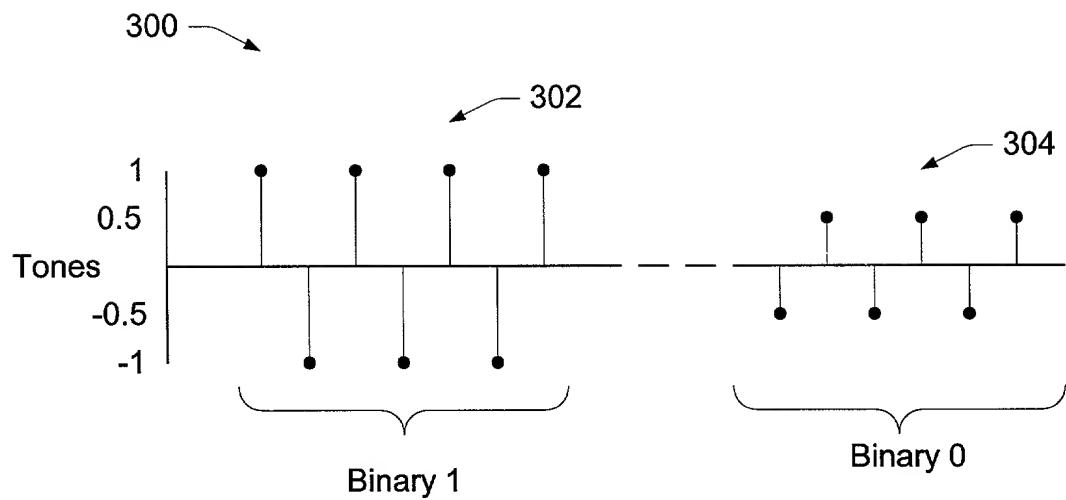


Fig. 6

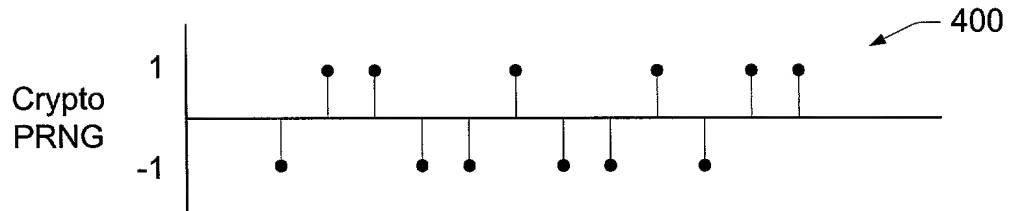


Fig. 7

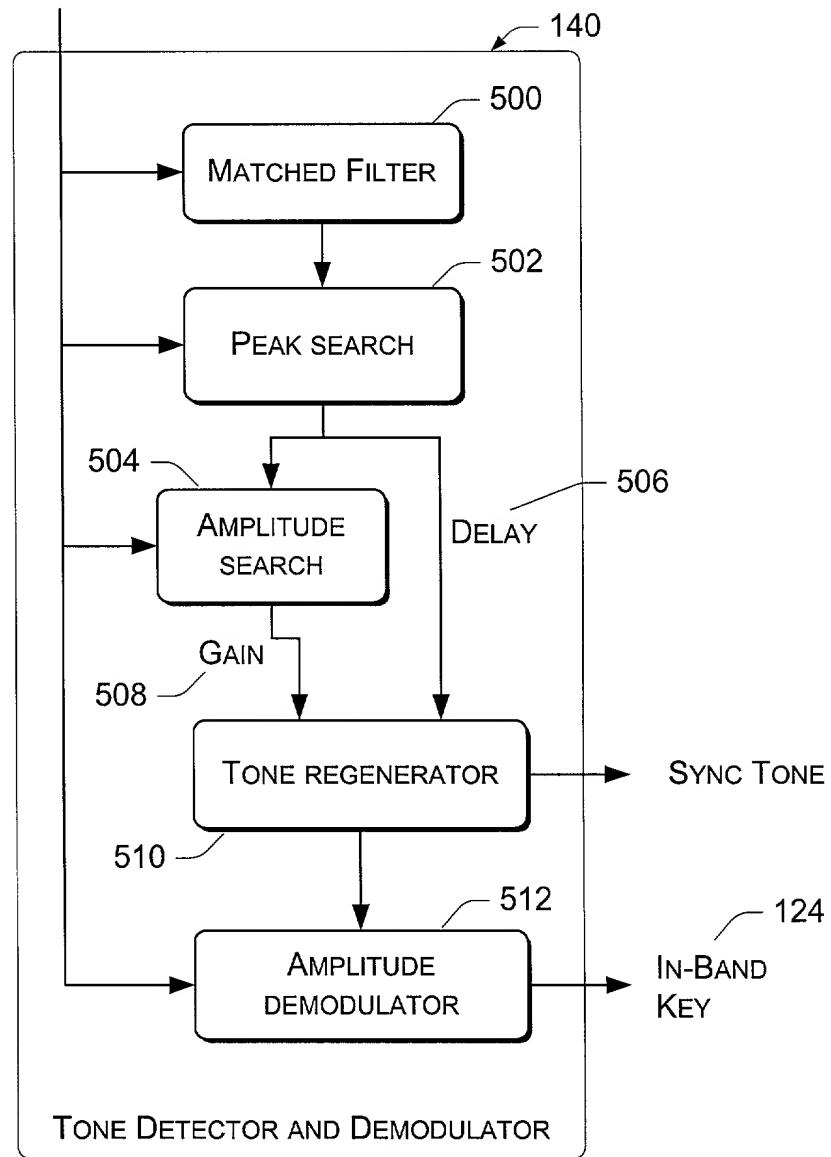
MODIFIED
NOISY DATA

Fig. 8

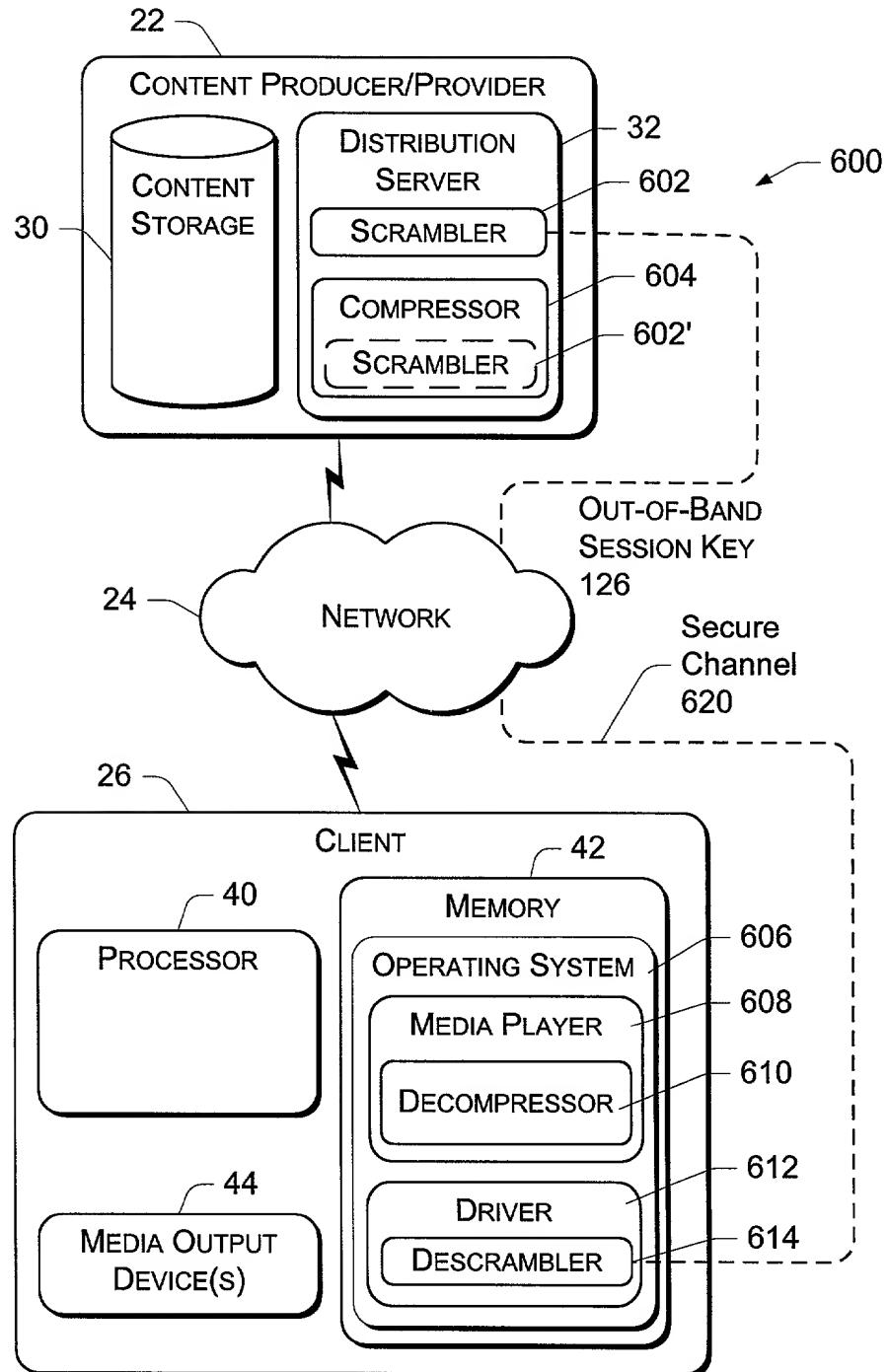


Fig. 9